



vPro

Benutzerhandbuch

Version R9

Deutsch

März 19, 2015

Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at <http://www.kaseya.com/legal.aspx>. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

Inhalt

vPro Überblick	1
vPro Modulvoraussetzungen	1
Automatische Einrichtung.....	1
vPro-Proxy	2
Verwalten von Boot-ISOs.....	4
Ermitteln und aktivieren.....	4
Drahtlos	6
Benachrichtigungen	7
Energie.....	9
Agentless Power Control	10
Remote Control.....	10
KVMView.....	11
Nach BIOS starten	12
Booten von ISO	12
Bonusformular	13
Protokolle	13
Inhaltsverzeichnis	15

vPro Überblick

Die Remote-Aktivierung von vPro-Rechnern erfolgt über **vPro**. Dazu gehören: Hochfahren, Herunterfahren von Windows, erzwungenes Herunterfahren, Abrufen/Ändern des vPro-Kennworts, Fernsteuerung nicht reagierender Rechner mithilfe von KVM, nach BIOS starten und Booten von ISO. Eine Funktion namens ‚vPro-Proxy‘ ermöglicht den Zugriff auf Rechner hinter einer Firewall sowie die Umgehung der Firewall und das Starten einer Remote-Sitzung durch Eingabe eines Zustimmungscodes, der nur lokal auf dem vPro-Rechner angezeigt wird. **vProOptional** kann vPro Befehle zum Hoch- und Herunterfahren an vPro-Rechner ohne Agents senden, die vom **Discovery**-Modul ermittelt wurden. Zudem kann vPro Rechner ohne Agents auch anhand deren IP-Adresse ermitteln und hochfahren.

vPro Modulvoraussetzungen

Kaseya Server

- Das vPro R9-Modul erfordert VSA R9.
- Eine Installation ist erforderlich. Die Nutzung wird auf Anfrage durch den Kundendienst freigeschaltet.

Anforderungen eines vPro-Proxys

- Der vPro-Proxy erfordert 200 MB freien Speicherplatz
- Microsoft .NET Framework 3.5

Hinweis: Siehe allgemeine **Systemanforderungen**

(<http://help.kaseya.com/WebHelp/EN/VSA/9000000/reqs/index.asp#home.htm>).

Automatische Einrichtung

vPro > Einrichtung > Automatisch

Die Seite **Automatisch** ermittelt und aktiviert vPro-Rechner. Die automatische Einrichtung kann gestartet oder auch nach einer Unterbrechung fortgesetzt werden. Es kann beispielsweise passieren, dass Sie die Einrichtung starten, aber den Browser schließen, bevor die Einrichtung abgeschlossen ist. Klicken Sie in diesem Fall auf die Schaltfläche **Fortsetzen**, damit die Einrichtung eines Rechners an dem Punkt fortgesetzt wird, an dem sie unterbrochen wurde.

Die automatische Einrichtung beinhaltet auch die Konfiguration von **vPro-Proxys** entsprechend den Anforderungen des ermittelten Netzwerks. Bei vPro-Proxy-Rechnern handelt es sich um Agent-Rechner, die vPro-Befehle zwischen dem VSA und den vPro-Rechnern übermitteln, die demselben Netzwerk angehören wie der Proxy-Rechner. Es wird für jedes Netzwerk, an das Sie vPro-Befehle zum Hoch- und Herunterfahren senden möchten, ein **vPro-Proxy** (siehe 2) benötigt. Außerdem ist ein vPro-Proxy erforderlich, um Rechner fernsteuern zu können.

Aktionen

- **Neuen Assistenten starten** – Klicken Sie, um den **Assistenten zur automatischen Ermittlung und Aktivierung von vPro-Rechnern** zu starten.

- **Seite 1 des Assistenten** – Wählen Sie diejenigen Rechner aus, die Sie auf vPro-fähige Chipsätze prüfen wollen, die bisher noch nicht ermittelt worden sind. Optional können Sie das Kontrollkästchen **Bereits ermittelte Rechner anzeigen** aktivieren.
- **Seite 2 des Assistenten** – Akzeptieren oder ändern Sie für jeden ermittelten vPro-Rechner den ausgewählten Agent-Rechner im selben Netzwerk, der als vPro-Proxy-Rechner wirken soll. Ein vPro-Proxy-Rechner muss nicht unbedingt ein vPro-fähiger Rechner sein. Er muss lediglich dazu in der Lage sein, vPro-Befehle an vPro-fähige Rechner im selben Netzwerk übermitteln können.
 - ✓ **Neu zuweisen** – Weisen Sie alle Rechner, die bereits einem Proxy zugewiesen sind, neu zu.
 - ✓ **Proxy ändern** – Weisen Sie einen einzelnen Rechner einem neuen Proxy zu.
- **Seite 3 des Assistenten** – Konfigurieren Sie die Agent-Rechner, die Sie als vPro-Proxy-Rechner ausgewählt haben. Geben Sie den Port an, den der vPro-Proxy nutzen soll, um nach **KVMView** (siehe 11)-Sitzungen zu lauschen, die von einem Administrator vom VSA aus gestartet wurden. Stellen Sie sicher, dass alle Firewalls und Router, hinter denen sich der vPro-Proxy befindet, dieselbe Port-Nummer geöffnet haben.
 - ✓ **Ändern** – Bearbeiten Sie die Port-Nummer.
 - ✓ **Bestätigen steht an** – Testen Sie die Verbindung zwischen dem VSA und dem vPro-Proxy.
- **Seite 4 des Assistenten** – Prüfen Sie den Status des laufenden Ermittlungs- und Aktivierungsvorgangs. Diese Seite wird automatisch aktualisiert.

Nicht abgeschlossene Assistenten

Unter **Nicht abgeschlossene Assistenten** sehen Sie den Status der **automatischen Einrichtung** von Rechnern, deren Einrichtung bisher nicht abgeschlossen wurde.

- **Aktuelle Seite** – Die aktuelle Seite des Assistenten.
- **Rechner-ID-FilterRechnergruppe** – Die Rechner-ID/Gruppen-ID eines Agent-Rechners.
- **Ansicht** – Die vom Administrator verwendete Ansicht zum Zeitpunkt, als die **automatische Einrichtung** unterbrochen wurde.
- **Scope** – Der vom Administrator verwendete Scope zum Zeitpunkt, als die **automatische Einrichtung** unterbrochen wurde.
- **Admin** – Der Administrator, der die **automatische Einrichtung** zum dem Zeitpunkt, als sie unterbrochen wurde, ausgeführt hat.
- **Datum** – Datum und Uhrzeit der Unterbrechung der **automatischen Einrichtung**.
- **Fortsetzen** – Klicken Sie, um die **automatische Einrichtung** des ausgewählten Rechners fortzusetzen.

vPro-Proxy

vPro > Einrichtung > vPro-Proxy

Auf der Seite **vPro-Proxy** können Sie:

- aus einem Agent-Rechner einen vPro-Proxy machen. vPro-Rechner, die sich im selben lokalen Netzwerk (LAN) befinden wie der vPro-Proxy-Rechner, werden diesem vPro-Proxy automatisch zugewiesen. Nach der Erstellung des vPro-Proxys wird dieser mithilfe der Option **Konfigurieren Sie vPro-Proxy** konfiguriert.
- Ausgewählte Rechner manuell einem anderen als dem automatisch zugewiesenen vPro-Proxy-Rechner zuweisen.
- den vPro-Proxy entfernen.

Ein vPro-Proxy ist ein Agent-Rechner, der eine Verbindung zu vPro-Rechnern herstellt. Ein vPro-Proxy wird in folgenden Fällen benötigt:

- Die vPro-Zielrechner befinden sich hinter einer Firewall und Sie möchten diese Rechner aus der Ferne (remote) hochfahren oder das Herunterfahren erzwingen. Der vPro-Proxy befindet sich im selben lokalen Netzwerk (LAN) und erfordert keine zusätzliche Konfiguration.
- Die vPro-Zielrechner befinden sich hinter einer Firewall und Sie möchten über **KVM** (siehe 11) eine Verbindung zu diesen Rechnern herstellen. Der vPro-Proxy befindet sich im selben lokalen Netzwerk (LAN) und ist mit einer öffentlichen IP-Adresse und einem öffentlichen Port konfiguriert. Diese öffentliche IP-Adresse und den öffentlichen Port teilen Sie dem VSA über den Dialog **Konfigurieren Sie vPro Proxy** mit.
- Sie möchten vPro-Zielrechner über KVM aktivieren, ohne jedes Mal einen Zustimmungscodes eingeben zu müssen, wenn eine KVM-Sitzung gestartet wird. Der vPro-Proxy nutzt denselben DNS-Server wie die Zielrechner und verfügt über ein korrekt konfiguriertes Zertifikat. Das Zertifikat wird nur verwendet, wenn der vPro-Rechner aktiviert ist. Danach starten KVM-Sitzungen ohne Eingabe eines Zustimmungscodes.

Es kann immer nur eine **KVMView** (siehe 11)-Sitzung pro vPro-Proxy aktiv sein. Der vPro-Proxy erfordert Windows XP oder eine neuere Windows-Version und muss nicht unbedingt ein vPro-Rechner sein.

Konfigurieren eines vPro-Proxys

1. Wählen Sie einen Rechner aus und klicken Sie auf **Einen vPro-Proxy erstellen**.
2. Klicken Sie auf die Schaltfläche **Konfigurieren**, die diesem Rechner zugeordnet ist.
3. Konfigurieren Sie die drei Abschnitte des Dialogs **Konfigurieren Sie vPro Proxy** unabhängig voneinander.
 - **Zertifikatserver** – Aktivieren Sie dieses Kontrollkästchen, wenn Sie **auf dem vPro-Proxy-Rechner ein Sicherheitszertifikat konfiguriert** (<https://helpdesk.kaseya.com/entries/33171573>) haben.
 - **KVM Proxy** – Geben Sie die öffentliche IP-Adresse und den öffentlichen Port des vPro-Proxys ein. Diese Informationen sind erforderlich, wenn Sie mithilfe von **KVMView** (siehe 11) eine Verbindung zu vPro-Rechnern herstellen möchten, die sich hinter einer Firewall befinden.
 - **Remote ISO** – Wählen Sie aus den diesem vPro-Proxy zugewiesenen ISO-Dateien diejenigen aus, **von denen vPro-Rechner booten sollen** (siehe 4).

Aktionen

- **vPro-Proxy erstellen** – Hierdurch wird in der Spalte **Konfigurieren** der ausgewählten Rechner zusätzlich die Schaltfläche **Konfigurieren** angezeigt. Klicken Sie die Schaltfläche **Konfigurieren** an, um die vPro-Proxy-Einstellungen für den jeweiligen Rechner zu konfigurieren.
- **vPro-Proxy entfernen** – Entfernen Sie vPro-Proxy-Einstellungen von den ausgewählten Rechnern.
- **vPro-Proxy testen** – Testen Sie die Verbindung zu ausgewählten vPro-Proxy-Rechnern.

Tabellenspalten

- **Rechner-ID** – Die Rechner-ID eines Agent-Rechners.
- **Ist vPro-Proxy** – Yes, wenn dieser Rechner bereits ein vPro-Proxy ist. Anderenfalls werden in dieser Spalte beispielsweise folgende Meldungen angezeigt:
 - Set Credential Account required for vPro Proxy Siehe **Anmeldedaten eingeben** (<http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#352.htm>).
 - vPro Proxy is only supported on Windows operating systems
 - Windows XP or alter is required for vPro Proxy
- **Zertifikat vorhanden** – Yes, wenn das System über ein vPro-Zertifikat verfügt.
- **KVM Proxy-IP** – Die IP-Adresse, die genutzt wird, um eine Verbindung zum vPro-Proxy herzustellen.
- **KVM Proxy-Port** – Der Port, der genutzt wird, um eine Verbindung zum vPro-Proxy herzustellen.

- **Konfigurieren** – Klicken Sie in einer Zeile auf die Schaltfläche **Konfigurieren**, um die vPro-Proxy-Einstellungen für den jeweiligen Rechner zu ändern.
- **Letzte Überprüfung** – Datum und Uhrzeit der letzten Überprüfung der vPro-Proxy-Verbindung.
- **Letztes Überprüfungsergebnis** – Das Ergebnis der letzten Überprüfung.

Verwalten von Boot-ISOs

vPro > Einrichtung > Boot-ISOs verwalten

Auf der Seite **Boot-ISOs verwalten** können Sie ISOs auf Ihren Kaseya Server laden. vPro-Rechner können Sie über die Seite **Remote Control** (siehe 10) von ISOs booten.

Hinweis: Befindet sich der vPro-Zielrechner hinter einer Firewall, ist ein **vPro-Proxy** (siehe 2) erforderlich.

Konfiguration

1. Laden Sie ISO-Dateien auf Ihren Kaseya Server, indem Sie >vPro > Einrichtung **Boot-ISOs verwalten** auswählen.
2. Klicken Sie die Schaltfläche **ISO hinzufügen** an. Suchen Sie nach der ISO-Datei, die Sie hochladen möchten.

Hinweis: Ist einem vPro-Rechner ein vPro-Proxy zugewiesen, muss die ISO-Datei über die Seite **vPro-Proxy** (siehe 2) auf den vPro-Proxy-Rechner hochgeladen werden.

3. Nutzen Sie die Seite vPro > **Remote Control** (siehe 10), um **von einer ISO-Datei zu booten**.

Hinweis: Weitere Informationen zum Hochladen großer ISO-Dateien finden Sie in der **Kaseya-Knowledge Base** (<https://helpdesk.kaseya.com/entries/35998997>).

Aktionen

- **ISO hinzufügen** – Lädt eine ISO-Datei hoch auf Ihren Kaseya Server
- **Entfernen** – Entfernt eine ISO-Datei von Ihrem Kaseya Server.

Tabellenspalten

- **Name** – Der Name einer bereits hochgeladenen ISO-Datei.
- **Beschreibung** – Eine Beschreibung der ISO-Datei.
- **Größe** – Die Größe der ISO-Datei in Megabyte.
- **Datum** – Datum und Uhrzeit, zu dem bzw. zu der die ISO-Datei hochgeladen wurde.

Ermitteln und aktivieren

vPro > Einrichtung > Ermitteln und aktivieren

Die Seite **Ermitteln und aktivieren** zeigt Rechner mit vPro-fähigem Chipsatz an, die ermittelt werden konnten. Sobald ein solcher Rechner ermittelt wurde, kann **vPro** einen Befehl zum Aktivieren bzw. Deaktivieren von vPro auf diesem Rechner ausgeben. Bei vPro-fähigen Rechnern können Sie diese Seite auch nutzen, um manuell einen **vPro-Proxy** (siehe 2) zuzuweisen. Zudem haben Sie die Möglichkeit, für vPro-Rechner, die nicht durch Kaseya aktiviert wurden, ein bekanntes Kennwort einzugeben oder das Kennwort für vPro-Rechner einzugeben, die durch Kaseya aktiviert wurden.

Aktionen

- **Ermitteln** – Sehen Sie nach, ob ausgewählte Rechner mit einem vPro-Chipsatz ausgestattet und vPro-fähig sind.

Hinweis: Hilfe bei der Ermittlung der Versionen vPro-fähiger Rechner finden Sie unter <http://communities.intel.com/docs/DOC-2033> (<http://communities.intel.com/docs/DOC-2033>).

- **vPro aktivieren** – Aktivieren bzw. deaktivieren Sie vPro auf ausgewählten Rechnern. Ein vPro-Rechner muss aktiviert sein, damit die auf dieser Seite erläuterten Funktionen ausgeführt werden können. Ob ein vPro-Rechner von VSA aus remote aktiviert werden kann, hängt davon ab, welche Version von AMT auf dem vPro-Rechner installiert ist.
 - **AMT 6.0 oder älter** – vPro muss manuell aktiviert werden.
 - **AMT 6.1** – Die hostbasierte Konfiguration ist standardmäßig *deaktiviert*. Sobald Sie aktiviert wird, kann vPro durch einen Klick auf die Schaltfläche **vPro aktivieren** aktiviert werden.
 - **AMT 6.2** – Die hostbasierte Konfiguration *kann aktiviert werden*. Sobald Sie aktiviert wird, kann vPro durch einen Klick auf die Schaltfläche **vPro aktivieren** aktiviert werden.
 - **AMT 7.0 und höher** – Die hostbasierte Konfiguration ist standardmäßig *aktiviert*. Sie können vPro durch einen Klick auf die Schaltfläche **vPro aktivieren** aktivieren.
- **vPro deaktivieren** – Deaktivieren Sie vPro auf ausgewählten Rechnern.
- **vPro-Kennwort**
 - **Neues Kennwort zuweisen** – Setzen Sie ein bekanntes, vorhandenes Kennwort sowohl auf dem vPro-Rechner als auch in VSA zurück. Wird ein vPro-Rechner erstmals mithilfe von **vPro** aktiviert, werden automatisch übereinstimmende Kennwörter festgelegt.
 - **Bestehendes Kennwort eingeben** – Ist ein vPro-Rechner bereits aktiviert worden, bevor er von VSA ermittelt wurde, so gibt es bereits ein vPro-Kennwort. Verwenden Sie diese Option, um das passende vPro-Kennwort einzugeben.

Hinweis: In der Spalte **AMT-Kennwort** auf dieser Seite sind die vPro-Kennwörter aufgeführt, die einem Rechner zugewiesen sind.

- **vPro-Proxy manuell zuweisen** – Weisen Sie ausgewählte Rechner manuell einem anderen **vPro-Proxy** (siehe 2) zu.

Tabellenspalten

- **Rechner-ID** – Die Rechner-ID/Gruppen-ID des Agent-Rechners.
- **AMT-Version** – Die vom vPro-Rechner verwendete Version von Intel Active Management Technology (AMT).
- **Aktiviert** – Wenn mit einem Häkchen versehen, dann ist vPro auf dem Rechner aktiviert.
- **AMT-Kennwort** – Das AMT-Kennwort für den Zugriff auf den vPro-Rechner.
- **KVM-Kennwort** – Das diesem vPro-Rechner zugewiesene KVM-Kennwort.
- **KVM-Modus**
 - **Client-Kontrollmodus** – Wenn eine **KVMView** (siehe 11)-Sitzung gestartet wird, wird auf dem Bildschirm des Remote-Rechners ein nach dem Zufallsprinzip generierter Zustimmungscode angezeigt. *Sie benötigen also einen Benutzer vor Ort, der Ihnen den Code durchgibt.* Oder:
 - **Admin-Kontrollmodus** – Der Rechner wurde bereits aktiviert und mit einem vPro-Proxy verknüpft, der mit einem Sicherheitszertifikat konfiguriert ist. **Klicken Sie hier, um Anweisungen zur Konfiguration eines Sicherheitszertifikats für einen vPro-Proxy zu erhalten** (<https://helpdesk.kaseya.com/entries/33171573>). Mithilfe dieser erweiterten Funktion kann ein VSA-Benutzer eine KVM-Sitzung starten, ohne dass ihm ein Benutzer vor Ort einen Zustimmungscode durchgeben muss.

- **AMT-SKU** – Der AMT-Gerätetyp. Unterschiedliche AMT-SKUs unterstützen unterschiedliche vPro-Funktionsmerkmalsätze.
- **Verbundener vPro-Proxy** – Derjenige vPro-Proxy, der eine vPro-Verbindung zu diesem Rechner herstellt.
- **Ermittlungsdatum** – Datum und Uhrzeit, an dem bzw. der der vPro-Rechner ermittelt wurde.

Drahtlos

vPro > Setup > Drahtlos

Die Seite **Drahtlos** erstellt WiFi-Profilen und ordnet sie verwalteten vPro-Rechnern zu. Damit wird eine Verbindung mit vPro-Rechnern unter Verwendung von Drahtlosnetzwerken ermöglicht. Ein vPro-Rechner muss bereits über einen installierten Agent verfügen und aktiviert sein, um auf dieser Seite angezeigt werden.

Erstellen von WiFi-Profilen

Wählen Sie die Dropdown-Option **Neues Profil erstellen**. Geben Sie die folgenden Details für ein vorhandenes WiFi-Netzwerk ein, das verwendet werden kann, um eine Verbindung mit einem oder mehreren verwalteten vPro-Rechnern herzustellen.

- **Profilname** – Der Name des WiFi-Profiles.
- **SSID** – Der WiFi-Netzwerkname.
- **Sicherheitsmethode** – Keine, WEP, TKIP, CCMP
- **Authentifizierungsmethode**
 - Für None oder WEP Sicherheitsmethoden – Open System oder Shared Key
 - Für TKIP oder CCMP Sicherheitsmethoden – WPA PSK, WPA IEEE 802.1x, WPA2 PSK, WPA2 IEEE 802.1x
- **Kennwort** – Für alle Authentifizierungsmethoden außer Open System erforderlich.
- **Beschränken auf Kaseya-Gruppe** – Beschränkt Zuordnung dieses WiFi-Profiles auf vPro-Rechner in der angegebenen Organisation/Rechnergruppe.
- **Standard für Kaseya-Gruppe** – Legt dieses WiFi-Profil als Standardprofil für die angegebene Organisation/Rechnergruppe fest.

Aktionen

- **WiFi-Profil zuweisen** – Weist ein ausgewähltes WiFi-Profil ausgewählten vPro-Rechnern zu.
- **Neues Profil erstellen/<auswählen>/Vorhandenes Profil entfernen** – Dienst zum Erstellen, Auswählen oder Entfernen von WiFi-Profilen von dieser Seite.
- **Profil bearbeiten** – Bearbeitet ein vorhandenes WiFi-Profil.
- **Standardverbindung einrichten** – Legt die von Kaseya verwendete Standardverbindung zur Verbindung mit vPro-Rechnern fest, denen ein WiFi-Profil zugewiesen wurde.
 - Über WiFi verbinden
 - Über Ethernet verbinden
 - Verbindung mit automatischer Erkennung – Stellt eine Verbindung über Ethernet her, wenn eine IP-Adresse auf der Ethernet-Verbindung erkannt wurde, als die vPro-Erkennung das letzte Mal ausgeführt wurde. Stellt eine Verbindung über WiFi her, wenn keine IP-Adresse auf der Ethernet-Verbindung erkannt wurde.

Benachrichtigungen

vPro > Einrichtung > Benachrichtigungen

Auf der Seite **Benachrichtigungen** können Sie Benachrichtigungen erstellen, die Aufschluss darüber geben, ob ein vPro-Ereignis erfolgreich war oder fehlgeschlagen ist. Die Liste der auswählbaren Rechner-IDs basiert auf dem Rechner-ID-/Gruppen-ID-Filter und dem verwendeten Scope.

So erstellen Sie einen Alarm:

1. Aktivieren Sie beliebige dieser Kontrollkästchen, um bei Auftreten einer Meldungsbedingung die entsprechenden Aktionen auszuführen:
 - [Alarm erstellen](#)
 - [Ticket erstellen](#)
 - [Skript ausführen](#)
 - [E-Mail-Empfänger](#)
2. Legen Sie weitere E-Mail-Parameter fest.
3. Wählen Sie eine der folgenden Angaben aus:
 - [on vPro Power On Success](#)
 - [on vPro Power On Failed](#)
 - [on vPro Force Power Down Success](#)
 - [on vPro Force Power Down Failed](#)
4. Markieren Sie die Rechner-IDs, auf die die Alarmeinstellungen angewendet werden sollen.
5. Klicken Sie auf [Einstellen](#), um die Alarmeinstellungen auf die ausgewählten Rechner-IDs anzuwenden.

So kopieren Sie Alarmeinstellungen:

1. Wählen Sie [copy all settings from](#) aus.
2. Klicken Sie auf ([Klicken Sie zum Auswählen](#)), um den per **Desktop Policy** verwalteten Rechner auszuwählen, von dem Benachrichtigungseinstellungen kopiert werden sollen.
3. Markieren Sie die Rechner-IDs, auf die die Alarmeinstellungen angewendet werden sollen.
4. Klicken Sie auf [Einstellen](#), um die Alarmeinstellungen auf die ausgewählten Rechner-IDs anzuwenden.

Alarm erstellen

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird ein Alarm erstellt. Alarme werden in Monitor > Dashboard-Liste, Monitor > Alarmübersicht und Info Center > Reporting > Berichte > Protokolle > Alarmprotokoll angezeigt.

Ticket erstellen

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird ein Ticket erstellt.

Skript ausführen

Ist diese Option mit einem Häkchen versehen, wird ein Skripting ausgeführt, sobald eine Benachrichtigungsbedingung eintritt. Sie müssen den Link [Klicken Sie zum Auswählen](#) anklicken, um ein Skripting auszuführen. Optional können Sie die ID des Rechners ändern, auf dem das Skripting ausgeführt wird, indem Sie [den Rechner mit dem Benachrichtigungslink](#) anklicken.

E-Mail senden an

Ist diese Option aktiviert und es tritt eine Meldungsbedingung ein, werden E-Mails an die angegebenen E-Mail-Adressen gesendet.

Benachrichtigungen

- Wenn das Optionsfeld **Zur aktuellen Liste hinzufügen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die angegebenen E-Mail-Adressen hinzugefügt, ohne dass die zuvor zugewiesenen E-Mail-Adressen entfernt werden.
- Wenn das Optionsfeld **Liste ersetzen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die zuvor zugewiesenen E-Mail-Adressen durch die angegebenen E-Mail-Adressen ersetzt.
- Wenn Sie auf **Entfernen** klicken, werden alle E-Mail-Adressen entfernt, **ohne dass irgendwelche Meldungsparameter geändert werden**.
- E-Mails werden vom Kaseya Server direkt an die in der Meldung angegebene E-Mail-Adresse gesendet. Den **Absender** können Sie über 'System > Ausgehende E-Mail' festlegen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmelde-symbol bewegen, wird das Agent-Quick View-Fenster angezeigt.

-  Online, aber in Wartestellung bis zum Abschluss des ersten Audits
-  Agent online
-  Agent online und Benutzer gegenwärtig angemeldet.
-  Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
-  Agent ist gegenwärtig offline
-  Agent hat nie eing_checked.
-  Agent ist online, aber die Fernsteuerung wurde deaktiviert.
-  Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten Rechner.Gruppen-IDs basiert auf dem Rechner-ID-/Gruppen-ID-Filter und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > Scopes anzuzeigen.

Name der Benachrichtigung

Listet die für jede Rechner-ID möglichen Alarme auf.

Antworten

Der jedem Alarm für jede Rechner-ID zugewiesene ATSE-Antwortcode:

- A = **A**larm erstellen
- T = **T**icket erstellen
- S = **S**kript ausführen
- E = **E**-Mail-Empfänger

Auszuführendes Skript

Das Skript, das ausgeführt werden soll, wenn diese Benachrichtigungsbedingung eintritt.

Skript ausführen auf

Die Rechner-ID, auf der das Skript ausgeführt wird, wenn diese Benachrichtigungsbedingung eintritt.

E-Mail an

Eine kommagetrennte Liste von E-Mail-Adressen, an die Benachrichtigungen gesendet werden

Energie

vPro > Einrichtung > Energie

Die Seite **Energie** ermöglicht es Ihnen, die folgenden Aufgaben für ausgewählte vPro-Rechner auszuführen:

- Hochfahren
- Herunterfahren
- Abschalten erzwingen
- Hochfahren von Rechnern ohne Agents

Diese Aufgaben können entweder sofort oder zu einem geplanten Zeitpunkt ausgeführt werden.

Hinweis: Befinden sich die vPro-Zielrechner hinter einer Firewall, ist ein **vPro-Proxy** (siehe 2) zum Hochfahren erforderlich.

Aktionen

- **Jetzt ausführen**
 - **Hochfahren** – Fahren Sie den vPro-Rechner sofort hoch. Befindet sich der vPro-Zielrechner hinter einer Firewall, ist ein **vPro-Proxy** (siehe 2) erforderlich.
 - **Windows herunterfahren** – Fahren Sie den vPro-Rechner sofort herunter.
 - **Abschalten erzwingen** – Erzwingen Sie das sofortige Abschalten eines Rechners. Dies ist gleichbedeutend mit dem Ziehen des Steckers am Rechner. Befindet sich der vPro-Zielrechner hinter einer Firewall, ist ein **vPro-Proxy** (siehe 2) erforderlich.
 - **Rechner ohne Agent hochfahren** – Fahren Sie einen bekannten, vPro-fähigen Rechner ohne Agent hoch, indem Sie dessen IP-Adresse angeben. Sie müssen außerdem einen anderen Rechner auswählen, der als vPro-Proxy fungiert und den Befehl zum Hochfahren ausgibt. Siehe **Agentless Power Control** (siehe 10).
- **Planen** – Planen Sie die einmalige oder periodische Ausführung einer Aufgabe. Bei jeder Art der Wiederholung (einmal, minütlich, stündlich, täglich, wöchentlich, monatlich) werden weitere verfügbare Optionen angezeigt. Periodische Zeitplanung bedeutet, dass Sie Start- und Endtermine für die Wiederholung einstellen müssen.
 - **Hochfahren planen** – Legen Sie einen Zeitplan für das Hochfahren fest. Befindet sich der vPro-Zielrechner hinter einer Firewall, ist ein **vPro-Proxy** (siehe 2) erforderlich.
 - **Herunterfahren von Windows planen** – Legen Sie einen **Zeitplan** (siehe 9) für das Herunterfahren von Windows fest.
 - **Geplantes Hochfahren abbrechen** – Brechen Sie das geplante Hochfahren ab.
 - **Geplantes Herunterfahren von Windows abbrechen** – Brechen Sie das geplante Herunterfahren von Windows ab.
- **Ermittelten Bestand anzeigen** – Wenn diese Option mit einem Häkchen versehen ist, können Sie sich vPro-Rechner ohne Agent anzeigen lassen, die als Bestand gekennzeichnet sind und mithilfe von **Discovery** ermittelt werden konnten. **Agentless Power Control** (siehe 10) kann hochgefahren oder zum Herunterfahren gezwungen werden.

Tabellenspalten

- **Aktueller Benutzer** – Der derzeit am Betriebssystem des Rechners angemeldete Benutzer.
- **Nächstes Hochfahren** – Datum und Uhrzeit, zu dem bzw. der ein Rechner das nächste Mal hochgefahren wird.
- **Zeitplan für das Hochfahren** – Der Zeitplan für das wiederholte Hochfahren des Rechners.
- **Nächstes Herunterfahren von Windows** – Datum und Uhrzeit, zu dem bzw. der Windows das nächste Mal heruntergefahren wird.

- **Zeitplan für das Herunterfahren von Windows** – Der Zeitplan für das wiederholte Herunterfahren von Windows auf diesem Rechner.
- **AMT-Kennwort** – Das AMT-Kennwort für den Zugriff auf den vPro-Rechner.
- **Verbundener vPro-Proxy** – Derjenige vPro-Proxy, der eine vPro-Verbindung zu diesem Rechner herstellt.

Agentless Power Control

Agentless Power Control mithilfe von Discovery

vPro kann Befehle zum Hoch- und Herunterfahren an alle vPro-fähigen Rechner ohne Agent ausgeben, die mithilfe des **Discovery**-Moduls ermittelt werden konnten.

- Nachdem die vPro-fähigen Rechner in einem Netzwerk mithilfe eines **Discovery**-Scans ermittelt worden sind, werden diese vPro-Rechner ohne Agent auf der Seite vPro-Management angezeigt, wenn das Kontrollkästchen unter vPro > vPro-Aktionen > **Energie** (siehe 9) > **Ermittelten Bestand anzeigen** aktiviert wurde.
- Die mithilfe von **Discovery** ermittelten vPro-fähigen Rechner können – entweder je nach Bedarf oder nach einem bestimmten Zeitplan – hoch- und heruntergefahren werden.
- Ein vPro-Rechner muss nicht in **Discovery** „in einen Bestand aufgenommen werden“, damit er in **vPro** auf der vPro-Seite angezeigt wird.
- Der **Discovery**-Sondierungsrechner, der zur Ermittlung der vPro-fähigen Rechner verwendet wurde, dient als **vPro-Proxy** (siehe 2), vom dem aus Befehle zum Hoch- und Herunterfahren an die ermittelten Rechner ausgegeben werden.

Agentless Power Control mithilfe der IP-Adresse

Es ist auch möglich, einen Befehl zum Hochfahren an einen bekannten vPro-fähigen Rechner ohne Agent zu senden, ohne dass dieser mithilfe von **Discovery** ermittelt werden muss. Hierzu muss die IP-Adresse des Rechners angegeben werden. Der Befehl wird mithilfe der Option vPro > vPro-Aktionen > **Energie** (siehe 9) > **Rechner ohne Agent hochfahren** ausgegeben. Wählen Sie eine der folgenden Optionen aus:

- **Hochfahrbefehl über vPro-Proxy senden** – Da **Discovery** nicht zum Ermitteln des vPro-fähigen Rechners verwendet wurde, muss der Benutzer einen Agent-Rechner im selben Netzwerk als vPro-fähigen Zielrechner angeben, der als vPro-Proxy-Rechner fungieren soll. Der vPro-Proxy gibt den Hochfahrbefehl an den vPro-fähigen Rechner aus.
- **Hochfahren mittels IP-Adresse** – Die IP-Adresse des vPro-Zielrechners, den Sie hochfahren möchten.
- **AMT-Benutzername** – Der AMT-Benutzername für den Zugriff auf den vPro-Rechner.
- **AMT-Kennwort** – Das AMT-Kennwort für den Zugriff auf den vPro-Rechner.

Remote Control

vPro > Einrichtung > Remote Control

Die Seite **Remote Control** ermöglicht es Ihnen, Probleme mit nicht reagierenden Rechnern zu beheben oder diese zu starten. Befindet sich der vPro-Zielrechner hinter einer Firewall, ist ein **vPro-Proxy** (siehe 2) erforderlich.

Hinweis: Für Windows-Standardanmeldesitzungen bietet **Kaseya Remote Control** (<http://help.kaseya.com/webhelp/DE/VSA/9000000/index.asp#17978.htm>) eine schnellere Verbindung.

Aktionen

- **Remote Control** – Führt eine **KVMView** (siehe 11)-Sitzung aus.
- **Nach BIOS starten** – Bootet den vPro-Rechner, um während einer KVMView-Sitzung **auf das BIOS zuzugreifen** (siehe 12).
- **Booten von ISO** – Bootet den vPro-Rechner von **einer Liste von ISOs** (siehe 12).

KVMView

KVM (Keyboard-Video-Mouse) steht für die Tastatur-, Video- und Maus-Fernsteuerung eines vPro-Rechners, die auch dann möglich ist, wenn das Betriebssystem des Rechners noch nicht installiert ist oder nicht ordnungsgemäß funktioniert. Eine KVM-Sitzung wird gestartet, wenn einer der folgenden **vPro**-Befehle ausgeführt wird:

- **Nach BIOS starten** (siehe 12)
- **Booten von ISO** (siehe 4)
- **vPro-Remote Control** (siehe 10)

KVMView

Bei KVMView handelt es sich um eine Anwendung zur Verwaltung der KVM-Verbindung zwischen dem Rechner des VSA-Benutzers und dem vPro-Zielrechner. Voraussetzung ist die Installation von KLC-Plugins. Möglicherweise werden Sie von Ihrem Browser aufgefordert zu bestätigen, dass **KVMView** gestartet werden soll. Sie haben in der Regel die Möglichkeit auszuwählen, dass diese Aufforderung beim nächsten Start einer KVM-Sitzung übersprungen werden soll.

KVMView-Zugriff über einen vPro-Proxy

Befindet sich der vPro-Zielrechner hinter einer Firewall, ist zur Ausführung einer KVMView-Sitzung ein vPro-Proxy (siehe 2) erforderlich. Außerdem muss der vPro-Proxy über eine öffentliche IP-Adresse und einen öffentlichen Port verfügen. Die öffentliche IP-Adresse und den öffentlichen Port des vPro-Proxys können Sie auf der Seite > Einrichtung > **vPro-Proxy** festlegen.

vPro-Sicherheit

Das Starten einer KVM-Sitzung erfordert entweder:

- die Eingabe eines nach dem Zufallsprinzip generierten Zustimmungscodes, der auf dem Monitor des Remote-Rechners angezeigt wird. *Sie benötigen also einen Benutzer vor Ort, der Ihnen den Code durchgibt.* Oder:
- Der Rechner wurde bereits aktiviert und mit einem vPro-Proxy verknüpft, der mit einem Sicherheitszertifikat konfiguriert ist. **Klicken Sie hier, um Anweisungen zur Konfiguration eines Sicherheitszertifikats für einen vPro-Proxy zu erhalten** (<https://helpdesk.kaseya.com/entries/33171573>). Mithilfe dieser erweiterten Funktion kann ein VSA-Benutzer eine KVM-Sitzung starten, ohne dass ihm ein Benutzer vor Ort einen Zustimmungscodes durchgeben muss.

KVMView – Aktionen

- **Datei**
 - **Beenden** – Schließt die **KVMView**-Anwendung.
- **Verbindung wird hergestellt**
 - **Start** – Baut eine **KVMView**-Verbindung auf.
 - **Stopp** – Beendet die **KVMView**-Verbindung.
 - **Aktualisieren** – Aktualisiert die Anzeige des Hostcomputer-Desktops.
 - **Farbqualität** – Legt die Farbqualität für das **KVMView**-Fenster fest: **Maximum**, **Medium**, **Low**.

- **Video skalieren** – Wird diese Option ausgewählt, wird die Größe des gesamten vPro-Desktops so angepasst, dass dieser in das **KVMView**-Fenster passt. Ist diese Option nicht ausgewählt, wird ein Ausschnitt des vPro-Desktops in voller Größe im **KVMView**-Fenster angezeigt.
- **Vollbild** – Ist diese Option ausgewählt, wird das **KVMView**-Fenster im Vollbildmodus angezeigt.
- **Werkzeuge**
 - **Strg-Alt-Entf senden** – Sendet den Befehl ‚Strg-Alt-Entf‘ an den Hostcomputer. (Das Drücken dieser Tastenkombination wird vom Client-Computer übersetzt.)
 - **IDET-Sitzung senden** – Startet eine ‚Booten von ISO‘-Sitzung.
 - **Optionen** – Nicht aktiviert, falls bereits eine Verbindung besteht.

Nach BIOS starten

Nach der Aktivierung eines vPro-Rechners können Sie den vPro-Rechner booten, und im Rahmen einer **KVMView** (siehe 11)-Sitzung auf das BIOS zugreifen. Befindet sich der vPro-Zielrechner hinter einer Firewall, ist ein **vPro-Proxy** (siehe 2) erforderlich.

1. Klicken Sie für einen bestimmten Rechner die Schaltfläche **Nach BIOS starten** auf der Seite vPro > vPro-Aktionen > **Remote Control** (siehe 10) an.
2. **Wenn der Rechner noch keinem vPro-Proxy zugewiesen ist oder der zugeordnete vPro-Proxy nicht mit einem Sicherheitszertifikat konfiguriert ist**
(<https://helpdesk.kaseya.com/entries/33171573>):
 - Geben Sie einen Zustimmungscod ein. *Sie benötigen also einen Benutzer vor Ort, der Ihnen den Code durchgibt.*
 - Klicken Sie die Schaltfläche **Ich habe authentifiziert** an, die in VSA in einem Pop-up-Fenster angezeigt wird, um fortzufahren.
3. Greifen Sie auf das BIOS des vPro-Zielrechners zu, der im **KVMView**-Fenster angezeigt wird.

Booten von ISO

Nach der Aktivierung eines vPro-Rechners können Sie den vPro-Rechner von einer ausgewählten ISO-Datei booten.

- Sie müssen die ISO-Datei zuvor über die Seite **Boot-ISOs verwalten** (siehe 4) auf den Kaseya Server hochgeladen haben.
- Befindet sich der vPro-Zielrechner hinter einer Firewall, ist ein **vPro-Proxy** (siehe 2)-Rechner erforderlich. In diesem Fall müssen Sie die ISO-Datei auch auf den vPro-Proxy-Rechner hochladen.

Booten von einer ISO-Datei

1. Klicken Sie für einen bestimmten vPro-Rechner die Schaltfläche **Booten von ISO** auf der Seite vPro > vPro-Aktionen > **Remote Control** (siehe 10) an.
2. Wählen Sie eine ISO-Datei aus der Liste hochgeladener ISOs aus.
3. Klicken Sie auf **Booten von ISO**.

Bonusformular

vPro > Einrichtung > Bonusformular

Kaseya nimmt an einem von Intel angebotenen vPro-Bonusprogramm teil. Wählen Sie vPro-fähige Rechner auf dieser Seite aus und klicken Sie dann diese Option an. Falls der jeweilige vPro-Rechner für einen Bonus in Frage kommt, können Sie umgehend eine CSV-Datei mit denjenigen Informationen erstellen, die Sie benötigen, um Ihren Bonusanspruch gegenüber Intel zu dokumentieren. Ein Link zu den **Regeln des Intel® vPro™ Channel-Partner-Programms**

(http://www.intel.com/cd/channel/reseller/asm-na/eng/products/platforms/vpro_activate/index.htm) liefert Ihnen nähere Informationen dazu, unter welchen Voraussetzungen Sie Anspruch auf einen Bonus haben.

Aktion

- **Bonusformular erzeugen** – Lädt eine CSV-Datei für ausgewählte Rechner herunter, die für einen Bonus in Frage kommen.

Protokolle

vPro > Verwaltung > Protokolle

Die Seite **Protokolle** zeigt ein Protokoll für einen verwalteten vPro-Rechner an.

- Ereigniszeit
- Ereignistyp

Inhaltsverzeichnis

A

Agentless Power Control • 10
Automatische Einrichtung • 1

B

Benachrichtigungen • 7
Bonusformular • 13
Booten von ISO • 12

D

Drahtlos • 6

E

Energie • 9
Ermitteln und aktivieren • 4

K

KVMView • 11

N

Nach BIOS starten • 12

P

Protokolle • 13

R

Remote Control • 10

V

Verwalten von Boot-ISOs • 4
vPro Modulvoraussetzungen • 1
vPro Überblick • 1
vPro-Proxy • 2